



RANTS & RAVES

Mel Croucher finds that Christmas has come early courtesy of the Chancellor of the Exchequer, while **Simon Edwards** attempts to rebuild his trust in his PC after he discovers it's been telling him porkies

GOLDEN BROWN

Mel Croucher **RAVES**

Last night I dreamed of a thick-set, one-eyed Scotsman. He was dressed up as Father Christmas and smiling like a battered cod. I queued outside his grotto with lots of other little boys and girls, and our excitement mounted as he doled out gifts to each tiny tot.

When it was my turn, he sat me on his knee and told me I had been a good wee lad. I hadn't told lies on my tax returns and I'd voted tactically against the Wicked Goblin

Party, allowing his New Reindeer Party to return to office with a reduced but significant majority. Then he rummaged in his big red attaché case to find my present. It was a state-of-the-art £1,500 computer! Santa said I could take it home and do what I liked with it. And I didn't have to worry if mummy and daddy could afford it, because Santa's Workshop would underwrite the costs over three years, no strings attached. And then I woke up.

I woke up to the fact that Gordon Brown has introduced an incredibly generous, astoundingly far-sighted and amazingly useful tax-

break for anyone who is employed in the UK. The Home Computing Initiative takes advantage of tax-exempt loan schemes that the Chancellor introduced back in 1999, and if your employer isn't using it as part of your benefits package, then you should damn well ask why.

A typical perk allows £1,500-worth of gear over three years, which should cover just about anything on offer in the pages of *Shopper*, fully warranted and from a trusted source. There's no deposit to pay, no credit check and the option to fund things at a couple of quid a month through so-called 'salary sacrifice'.

Technically, it's a glorified loan, but at the end of your loan period you can buy the gear at a nominal market price, which the Chancellor interprets as about a tenner.

MANY HAPPY RETURNS

I expect Gordon Brown has got a hidden agenda – probably a scheme to get us all filling in tax returns online from home – but the rules clearly state that we can use our new PCs and flat-screen displays for anything we like, including watching DVDs and playing online poker. We could even use them to look for a new job, so our next employer can give us another new machine, as there is no limit to the number of computers we are allowed as long as we stick to the annual limits.

Until recently, only 500 or so firms had taken advantage of the scheme, but now the Department of Trade and Industry has published clear guidelines and expanded the system to cover the public sector, too, which is good news for nurses, teachers and council workers.

I'd like to see Brown extend his largesse to cover the retired, self-



employed and unemployed, but this wouldn't be *Rants & Raves* unless I had some sort of quibble. Oh all right then, let's break the rules for once. Thanks Santa, you're a gent.

KANGAROO COURT

Simon Edwards

RANTS

When a young Korean woman boarded a train with her pet dog, little did she know her life was about to change for the worse. It wasn't that she minded when the little scamp did a poo (and, dare we say it, a fairly sloppy one at that) on the floor of the carriage, or that other passengers remonstrated with her to clean it up. She didn't care about that, and left the mess where it was.

She was more worried when pictures of her sitting on the train next to the dog and its business were published on the internet. Someone on the train had used a mobile phone camera to capture her disgrace. Within days her identity was established, and published too.

This internet-based public shaming led to her leaving university.

When Dan Hoyt exposed himself to a woman on a New York train he probably wasn't expecting anyone to take a photo of him. Or that they would publish the picture on the web, that the police would become involved or that a newspaper would print a photo of his face. His identity was soon established and, on 2nd September, the Manhattan restaurateur left a courthouse having been charged with four counts of public lewdness.

Are these tales funny or sinister? It's hard to argue that Hoyt's privacy had been invaded when he was caught, shall we say, red-handed and being deeply unpleasant to young women. His reported arrogance at the court doesn't help, either. But kangaroo court systems, even on the internet, are not a great idea. When shame is the punishment, the shameless will get off free, while more vulnerable people will crumble.

DON'T LIE TO ME

Simon Edwards

RANTS

We all know that computers can be unreliable, but did you know that sometimes they actually lie to you? Just as a child with bad influences may become deceitful, a computer that has been attacked by a reasonably knowledgeable hacker will start to tell lies.

Imagine asking your PC to list all the files in your My Documents folder, but instead it gives an incomplete list, hiding a folder that contains some secret programs. Perhaps you want to know what network connections your PC has made to the internet? That would be useful to see what sites your PC has connected to, but also what computers are connected to you.

You can find out by running a diagnostic program such as netstat from the command line or download TCPView from www.sysinternals.com. Except that if your computer has learned to lie it will omit to tell you about the incoming connections from Eastern Europe.

My computer has started to lie, but I'm not angry. Just disappointed. It didn't want to do it – someone told it to. Nevertheless, I know it will take a while – and a good reinstalling – before I can start to build up a trusting relationship with it again.

So where does the rot start? Who are the bad influences that corrupt our pride and joys? The

answer is: rootkits. A rootkit is a piece of software designed to subvert your computer's operating system so thoroughly that it is unable to report its status accurately. It will tell you enough to keep you happily ignorant of an attack, so detecting a rootkit is tricky.

A rootkit is used by an attacker to hide their tracks. For example, if someone wanted to take over your PC they would probably want to store a few useful programs on your hard disk and make connections to and from your system across the internet. But the attacker faces some problems. If you have an anti-virus program and firewall software running on your PC he shouldn't be able to store well-known tools or even make connections without your permission.

But if the attacker can convince the very core of the operating system, known as the kernel, to play his way, then all of the security software installed on the system essentially becomes useless. Here's how it works.

On a compromised machine, an attacker could instruct the firewall to continue to work properly, except that it should allow connections from a certain address on the internet

CODE COMFORT

Simply put, when you run a program in Windows it talks to system files (known as DLLs) that contain the chunks of programming code it needs to run. This dialogue can be intercepted by an attacker, who can then manipulate the program being run by injecting his own code.

For example, on a compromised machine an attacker could instruct the firewall to continue to work properly, except that it should allow incoming connections from a certain address on the internet. This change won't appear in the program's control panel and you'll be none the wiser.

The same principle works on Linux computers, which have been exposed to this kind of hacking for longer than Windows systems. But just recently anti-virus companies have started to report an increase in the use of rootkits with Windows.

Kaspersky Lab says that "the increased popularity of rootkits is partly due to the fact that the source code of many rootkits is now openly available on the internet. It's relatively easy for virus-writers to make small modifications to such code."

It's no surprise, then, that the anti-virus companies have been investing time and money into detecting rootkits. The problem is, if the system has already been infected, any software you run on it could lie to you. Nevertheless, Kaspersky Lab's next release of its anti-virus software (version 6) is expected to include rootkit detection abilities, while F-Secure is currently allowing anyone to download and install a beta version of its BackLight rootkit detection utility. BackLight (www.f-secure.com/blacklight) is also built into its new Internet Security 2006 product.

PROTECT AND SERVE

This is no help to me, though, because my computer runs Linux. It's been sat on the internet for some time now, quietly posing as an innocent web server with a few extra bells and whistles. Some of these enable me to monitor what people are up to. This usually involves crude attempts to hack in by guessing the passwords, but one day I found that

someone had managed to log in. He was calling from a university in Budapest and, while I'm not allowed to tell you what he was up to, I can say that we kicked him off pretty sharpish.

The most interesting part of the exercise was examining the hacked system while the hacker was actually using it. Nothing appeared to be amiss, except that we knew he was logged in and yet couldn't see him in the list of logged-in users. The post-mortem revealed a Linux rootkit that was fooling the kernel into feeding us false information.

Sadly, unlike a lying child, it is virtually impossible to reform a PC that won't tell the truth. It is possible to reformat it, though, and that's what we've done. It's out there again now, waiting for baddies to connect so we can see what they're up to. ☹

CONTACT

MEL CROUCHER

mel@computershopper.co.uk

SIMON EDWARDS

simon@computershopper.co.uk